FORGEDOPS PLANS

Security Whitepaper

Identity, isolation, audit, and operational controls for the ForgedOps Plans platform. Prepared for procurement review by contractors, municipalities, state agencies, airports, utility owners, and enterprise SaaS customers.

Version 1.0 · Effective January 1, 2026

Last Updated · January 1, 2026

1 · Executive Summary

ForgedOps Plans is a multi-tenant, cloud-hosted construction plan-intelligence platform. This whitepaper documents the controls in place today and the roadmap for controls planned for the next pilot-to-commercial transition. ForgedOps does not claim certifications it does not hold; every claim in this document maps to an implementation in the production code base.

- Single-tenant boundaries enforced at every API call.
- JWT-based authentication with short-lived access tokens and rotated refresh tokens.
- Role-based access control over every administrative surface.
- All uploads validated by extension allowlist, magic-byte, macro-block, and size cap before storage.
- Encrypted in transit (TLS 1.2+) and at rest (Cloudflare R2).
- Tamper-evident audit logging on every security-relevant action.

2 · Platform Overview

ForgedOps Plans is delivered as a Software-as-a-Service application accessible from any modern browser. The platform hosts plan PDFs, field photos, project records, takeoffs, punch items, and exports. Customer data is stored in tenant-scoped namespaces in a managed MongoDB cluster and a Cloudflare R2 object store. The application server is FastAPI on Python, the front end is React. All traffic is served over HTTPS via Cloudflare.

3 · Security Architecture

The architecture follows defense in depth: the perimeter (TLS + Cloudflare), the application (authentication + RBAC + tenant isolation), and the data tier (tenant-scoped queries + encrypted storage). Each layer enforces controls independently so a single failure does not result in data exposure.

Layer	Primary control
Edge	TLS 1.2+ · HSTS · Cloudflare WAF
Application	JWT auth · RBAC · tenant guards
Storage	R2 SSE-S3 at rest · signed URLs · tenant-prefixed keys
Operations	Least-privilege ops · secret-store env · audit trail

4 · Identity & Access Controls

Authentication

All access is gated by a short-lived JWT access token. Tokens are issued on a successful POST to /api/auth/login and refreshed via POST /api/auth/refresh. Passwords are stored as salted bcrypt hashes — never logged, never returned by any endpoint. Failed logins are rate-limited and recorded in the audit log.

Roles & least privilege

Six tenant roles are enforced: Owner, Admin, Project Manager, Superintendent, Foreman, and Viewer. A separate platform-admin scope is gated by an explicit environment allowlist (PLATFORM_ADMIN_EMAILS) — no tenant role can reach platform endpoints. Write operations on sensitive resources require Owner or Admin; project create / update requires Owner / Admin / PM; sheet upload requires Owner / Admin / PM / Superintendent.

5 · Tenant Isolation

Every customer's data is partitioned by a tenant_id. Every API endpoint queries with the authenticated user's tenant_id; cross-tenant probes return 404 (the resource is hidden, not just denied). Storage keys are tenant-prefixed so a leaked object key cannot be replayed against a different tenant. Audit logs are also tenant-scoped — a tenant administrator only sees rows that belong to their tenant.

6 · Audit Logging

Every administrative, security-relevant, and data-changing action writes an immutable audit row capturing actor, action, target, IP address, user-agent, success/failure, severity, and a structured metadata payload. Audit retention is configurable up to seven (7) years.

- auth.login_success / login_failure
- tenant.user_invited · invite.email.sent · invite.email.failed
- tenant.invite_accepted · invite.revoked
- sheet.upload (success and failure with reason)
- document.upload_rejected (reason + filename + content-type + size)
- platform.tenant_created / tenant_disabled / tenant_archived

7 · File Security

Every upload endpoint validates content before storage. The validator checks extension against an allowlist, performs magic-byte verification (e.g. %PDF, JPEG, PNG, OOXML PK header), blocks executable and script extensions, and refuses macro-enabled Office documents (docm/xlsm/pptm). Files are stored under server-generated opaque filenames (token_hex(8) + detected extension) — the client-supplied filename is discarded to prevent path traversal and double-extension tricks. Rejected uploads are recorded with reason in the audit log.

8 · Data Ownership

Customer Data — plans, drawings, photos, project records, annotations, exports — remains the property of the customer. ForgedOps acts as a processor on the customer's behalf and stores Customer Data only as long as needed to operate the platform. ForgedOps does not sell, license, or share Customer Data with third parties for marketing or advertising. See the ForgedOps Data Ownership Statement for the full text.

9 · Data Privacy

The complete privacy policy is published at https://forgedopsplans.com/legal/privacy. Categories of information collected include account information, uploaded files, photos, drawings, project records, audit logs, browser / device information, usage analytics, cookies, and session tokens. ForgedOps uses strictly-necessary cookies only — no third-party tracking or advertising cookies are present.

10 · Storage Architecture

Customer files are written to Cloudflare R2, an S3-compatible object store with server-side encryption at rest. Objects are written to tenant-prefixed keys (tenants/<tenant_id>/projects/<project_id>/...). Direct anonymous access is denied at the bucket policy layer. Files are delivered to authenticated users via short-lived pre-signed URLs only. Credentials used to write storage are stored as environment secrets — never in source control.

11 · Backup & Recovery

The primary database is backed up on a daily schedule. Backups are retained on a rolling 90-day window. Object-store contents are versioned where supported by the provider. Restore procedures are documented in an internal runbook and exercised on a recurring cadence.

12 · Operational Security

- Production access is limited to authorized engineering personnel under principle of least privilege.
- All secrets — Resend, R2, JWT signing keys — are environment variables managed in the deployment platform.
- Every deployment is traceable to a specific source revision.
- Third-party services are vetted for security posture before integration; current vendors: Cloudflare (TLS / CDN / R2), Resend (email), Emergent platform (hosting).
- Security-relevant code paths are covered by automated regression tests (auth, tenant isolation, audit, upload validation).

13 · Support & Incident Response

Customers can reach the operator team at support@forgedopshq.com. Production-impacting issues are triaged the same business day; functional bugs within one business day; feature requests within

three business days. Security-sensitive vulnerabilities should be reported to security@forgedopshq.com or info@forgedopshq.com. Standard business hours are Mon–Fri, 8a–6p ET. The platform exposes anonymous health endpoints (/api/health, /api/system_health) for external monitoring.

14 · Security Roadmap

Current (live today)

- TLS 1.2+ for all traffic; HSTS enforced.
- JWT-based authentication with rotated refresh tokens.
- Role-based access control across all administrative surfaces.
- Multi-tenant isolation with tenant_id-scoped queries.
- Upload validation: extension allowlist + magic byte + macro block + size cap.
- Tamper-evident audit logging.
- Encrypted at-rest object storage (Cloudflare R2 SSE-S3).
- Daily database backups with 90-day rolling retention.

Planned (next 12 months)

- Malware signature scanning on uploads (ClamAV or cloud AV).
- Enhanced monitoring + alerting (SIEM-style aggregation).
- Single sign-on (SSO) via SAML 2.0 / OIDC for enterprise tenants.
- Compliance alignment (SOC 2 Type I scoping exercise).
- Customer-managed retention policies.

ForgedOps does not currently hold SOC 2, ISO 27001, FedRAMP, or HIPAA certification. Any future certification will be announced publicly on the Trust Center; we do not claim certifications we have not obtained.

15 · Contact Information

- Support · support@forgedopshq.com
- Information · info@forgedopshq.com
- Security · security@forgedopshq.com
- Web · https://forgedopshq.com
- Platform · https://forgedopsplans.com
- Trust Center · https://forgedopsplans.com/trust
- Legal · https://forgedopsplans.com/legal/terms · /legal/privacy · /legal/security

- Company · ForgedOps LLC